Observatoire du Monde Cybernétique

Janvier 2012

La Commission européenne veut réformer la protection des données en ligne

Le 25 janvier 2012, la Commission européenne a déposé un paquet de mesures destinées à réformer les règles de protection des données personnelles en ligne. La réforme, intitulée « Protection de la vie privée dans un monde en réseau : un cadre européen relatif à la protection des données, adapté aux défis du 21ème siècle », s'organise autour d'un règlement général sur la protection des données et d'une directive spécifique pour le domaine de la police et de la Justice.

***Blackout* Internet massif en contestation des lois SOPA et PIPA**

Suite à la révolte massive et au *blackout* de plusieurs sites Internet, les votes des lois américaines relatives au renforcement de la propriété intellectuelle *« Stop Online Piracy Act »* (SOPA) et *« Protect IP Act »* (PIPA), ont finalement été reportés *sine die*. Parmi les sites web mobilisés : AOL, eBay, Facebook, Google, LinkedIn, Mozilla, Twitter, Yahoo et surtout Wikipedia (sa version américaine) qui a rendu son site inaccessible pendant toute une journée.

Développement d'un virus capable de contrer les cyberattaques

Le Japon développerait depuis 3 ans un virus capable de remonter la source d'une attaque informatique et de la neutraliser. Cette « cyberarme » aurait été financée à hauteur de 179 millions de yen (2,3 millions de dollars) attribués par le gouvernement japonais à Jujitsu Ltd. La législation japonaise devrait être revue en conséquence pour autoriser la production et l'utilisation d'un tel virus informatique.

Un cheval de Troie pirate les *smartcards* du Département de la Défense américain

Une variante du cheval de Troie *Sykipot* susceptible de voler les détails de *smartcards* du *Department of Defense* américain aurait été découverte par les laboratoires de sécurité informatique Alien Vault. Celle-ci aurait déjà été utilisée dans une douzaine d'attaques et usurperait les données des *smartcards* du DoD afin d'accéder à des informations confidentielles.

Piratage de Symantec et fuite de code source de Norton Antivirus

Le groupe de *hackers* « The Lords of Dharmarâja » revendique la possession du code source de Norton Antivirus remontant à 2006 et l'a dévoilé le mardi 17 janvier 2012. Suite à cet incident, des failles non corrigées ont été découvertes dans leur suite *pcAnywhere*. Symantec a recommandé de désactiver le service jusqu'à publication d'une nouvelle mise à jour.

Le conflit arabo-israélien s'intensifie sur la toile

Les attaques en ligne continuent entre pirates israéliens et arabes. Après la divulgation de plus de 20 000 cartes de crédit israéliennes, des *hackers* israéliens ont répliqué en publiant des coordonnées bancaires saoudiennes. Les attaques se multiplient de part et d'autre. Fait marquant : le gouvernement israélien a déclaré considérer les attaques saoudiennes comme des actes terroristes.

Le « Kopimism » : une religion pour les h*ackers* ?

L'Eglise Missionnaire du Kopimisme (*« Missionary Church of Kopimism »,* dérivé de l'anglais « *copy me »*) née 2010, a été reconnue comme une religion officielle en Suède le 5 janvier 2012. « Cette religion a pour principale doctrine de partager et de diffuser des dossiers » sur Internet. L'église compterait déjà plus de 3 000 adeptes dans le monde.

Le cabinet ministériel ukrainien mettra au point un projet de loi relatif à la cybercriminalité

Le Conseil des Ministres de l'Ukraine présentera courant 2012 un projet de loi sur la cybercriminalité. Début décembre 2011, le Parlement avait déjà enregistré une proposition visant à compléter les articles du code pénal condamnant le piratage informatique.

La Biélorussie restreint l'accès aux sites web étrangers depuis son territoire

Une nouvelle loi posant *« des restrictions quant à l'utilisation et la consultation des sites web*

étrangers par les citoyens et résidents du pays » est entrée en vigueur le 6 janvier 2012 en Biélorussie.

Un projet de système de contrôle d'Internet en Russie suspendu

Le Service Fédéral Russe de Supervision des Télécoms avait lancé un appel d'offres pour un Système de Contrôle du Contenu de l'Internet, remporté par la société moscovite « Data Center ». Le système, qui devait rentrer en vigueur le 15 décembre 2011, n'a toujours pas été mis en place. Selon Ilya KOROBEINIKOV, le Directeur Général de Data Center, *« le Ministère n'a toujours pas accepté le système élaboré par notre société. Nous n'avons eu aucune explication ».* Par ailleurs, le 20 janvier 2012, le Ministre de la Communication, Igor CHEGOLEV avait rappelé : « *En Russie, l'Internet est plus libre que dans les pays occidentaux… On croit que le gouvernement russe veut avoir le contrôle total sur l'Internet mais, en réalité, on exclut la possibilité de bloquer l'accès aux réseaux sociaux comme Twitter ou Facebook comme le font les gouvernements européens* ».

Etats-Unis : Booz Allen Hamilton réorganise ses activités de cybersécurité

Booz Allen Hamilton a annoncé la création du *Cyber Solutions Network*, nouvelle ligne de produits de cybersécurité destinée à mutualiser l'ensemble de ses ressources en la matière pour la protection des réseaux informatiques de ses clients gouvernementaux et privés. La société va ainsi connecter ses neuf centres de cybersécurité, ses laboratoires et ses différents sites d'expertise au sein d'un réseau interconnecté. Celui-ci doit ainsi lui permettre de fournir des capacités d'analyse avancée des activités cyber, de défense des réseaux informatiques, de tests et d'évaluation de réseaux et de formation à la cybersécurité.

Telos sélectionnée pour l'opération et la maintenance de l'*Air Force Information Network*

Grâce au contrat-cadre *NETCENTS*, Telos a été sélectionnée comme principal prestataire pour l'exploitation et la maintenance de l'*Air Force Information Network* (*AFIN*) soutenant le *561st Network Operations Squadron* (*561 NOS*). Composé de services de communications filaires, sans fil et mobile, le réseau *AFIN* met en œuvre les spécifications *AFNetOps* pour les opérations du *561 NOS* auprès de nombreux commandements stratégiques américains dont l'*US Strategic Command* et l'*US Cyber Command*. Les équipes de Telos seront composées d'opérateurs de réseaux et de spécialistes de la sécurité, pour assurer la posture de sécurité et de continuité du réseau informatique du *561 NOS*.

La solution de cybersécurité WebShield de Raytheon certifiée pour le DoD et la communauté du renseignement

La solution de cybersécurité *WebShield* de Raytheon a été inscrite sur la liste des solutions et des technologies éligibles pour les programmes du DoD et de la communauté américaine du renseignement. Cette liste est gérée par l'*Unified Cross Domain Management Office*. *WebShield* est une solution de contrôle du trafic sécurisé HTTP pour l'accès à des réseaux informatiques comprenant différents niveaux de sécurité. Elle permettra de sécuriser les opérations de recherche et de navigation sur Internet à partir de réseaux hautement ou faiblement classifiés.

L'*US Air Force* publie une RFI pour concevoir sa stratégie cyber à l'horizon 2025

L'*US Air Force* a publié une *Request For Information* pour obtenir du secteur privé des connaissances sur l'état actuel de la R&D dans la cyberdéfense. Ces informations seront utilisées pour la rédaction de son étude *Air Force Cyber Vision 2025* devant établir à court, moyen et long terme, la vision de l'*US Air Force* concernant ses capacités de cyberdéfense. Ces informations sont jugées nécessaires pour l'élaboration de nouvelles stratégies, le développement de nouveaux logiciels, systèmes informatiques et procédures.

[McAfee & DBS] Cyber-security : The Vexed Question of Global Rules

Les sociétés *McAfee* et *Security & Defence Agenda* viennent de publier un rapport sur les cybermenaces et les mesures qui devraient être prises à leur encontre. A titre d'exemple, 57% des experts interrogés croient en une « course aux armements » dans le cyberespace.

[World Economic Forum] Davos report : Cyber-attack risk to global stability is real

D'après un rapport du *World Economic Forum* sur les risques globaux pour 2012, les attaques informatiques arriveraient en 5ème position des risques les plus présents. Ceci n'est pas nouveau pour les grands acteurs de l'industrie informatique, mais cela reste une menace nouvelle pour les gouvernements et autres entités non-spécialistes. La constante évolution de la technologie rendrait donc le panorama des risques liés à la cybercriminalité dur à suivre, d'autant plus que les retours sur le sujet divergent : les entreprises de sécurité multiplient les avertissements, alors que les victimes de cyber-attaques ont tendance à rester silencieuses.

[ENISA] Proactive detection of network security incidents, report

D'après un rapport de l'agence de cybersécurité européenne, l'ENISA, les CERT européens n'utiliseraient pas toutes les ressources à leur disposition pour implanter une détection proactive des incidents de cybersécurité, alors qu'ils déclarent être ouverts à l'adoption de nouvelles technologies. De plus, l'information entre CERT ne serait pas partagée de manière efficace, ce qui constitue un élément clé du combat contre les *malwares* et autres activités frauduleuses.

[DHS] Blueprint for a Secure Cyber Future

Le *Department of Homeland Security* a publié un rapport décrivant les grandes lignes de protection des infrastructures sensibles américaines face aux cybermenaces, en mettant en avant le rôle de leurs partenaires internationaux et des entreprises privées. Le rapport aborde deux thématiques : la protection actuelle des infrastructures d'information critiques et la construction d'un cyber-écosystème plus fort sur le long terme.

[Macdonald-Laurier Institute] Canada's critical infrastructure open to cyberattacks, warns think tank

Un rapport du *think tank* canadien *Macdonald-Laurier Institute* révèle que les infrastructures vitales du Canada seraient très vulnérables aux cyberattaques. Il affirme que le gouvernement canadien doit impérativement mettre en place un plan global visant à protéger ces infrastructures. Le rapport comprend une série de recommandations destinées au gouvernement fédéral : établir un inventaire précis des infrastructures critiques ; améliorer le partage de l'information ; éduquer le public sur les menaces ; aider financièrement le secteur privé pour l'inciter à protéger ses infrastructures critiques.

[The Cyber Hub] Cyberpower Index

Booz Allen Hamilton et le *Economist Intelligence Unit* ont publié les résultats d'une étude sur les cyber-puissances mondiales sous forme d'indicateurs interactifs. Le Royaume Uni et les Etats-Unis seraient les Etats *leaders* en matière de cyber-pouvoir et cyberéconomie. La France, elle, arriverait en 6ème position. Le barème tient compte des outils légaux, du contexte socio-économique, des infrastructures technologiques et de l'application des normes à l'industrie.

Retour sur la conférence du CLUSIF : panorama de la cybercriminalité

Comme chaque début année, le CLUSIF (Club de la Sécurité de l'Information Français) a présenté son bilan en matière de cybercriminalité et d'incidents liés à la sécurité de l'information. Une dizaine d'experts, adhérents du CLUSIF (dont des consultants de CEIS) mais aussi des spécialistes invités spécialement pour l'occasion, ont travaillé pendant plusieurs mois au sein d'un groupe de travail pour sélectionner les faits marquants de l'année 2011 et ceux qui auront de fortes répercussions en 2012.

Cette année, le Panorama de la Cybercriminalité s'est focalisé sur les thèmes suivants :

- **L'innovation dans la fraude aux moyens de paiement.** Les cybercriminels continuent de faire évoluer leurs techniques de fraude. En 2011, ils ont commencé à utiliser des kits de *skimming* créés par imprimante 3D. Le *carding* poursuit son industrialisation. La vente de cartes bancaires s'effectue via des sites spécialités en tout point semblables à des sites de e-commerce classiques.

- **Les menaces mobiles qui se précisent.** Après le GSM, c'est le protocole GPRS qui semble vulnérable. Les OS mobiles comme Android et iOS sont victimes de nombreuses failles. Les *malwares* se multiplient également sur ces plateformes mobiles (notamment sur Android). L'outil LOIC utilisé par les Anonymous pour lancer des dénis de service apparaît également sur Android.

- **L'impact de la compromission des autorités de certification sur la confiance sur Internet.** En 2011, deux autorités de certification (Comodo et DigiNotar) ont été compromises par un *hacker*, provoquant des risques d'usurpation d'identité et d'écoute des échanges. Selon certaines rumeurs, d'autres autorités auraient aussi été piratées. Des attaques qui mettent à mal le modèle de tiers de confiance sur Internet.

- **L'hacktivisme en 2011 : visée politique ou simples enfantillages ?** La montée en puissance de l'hacktivisme s'est confirmée en 2011. Les Anonymous et autres LulzSec ont marqué l'actualité par leurs nombreuses cyberattaques, essentiellement contre des entreprises et des gouvernements.

- **Les cybermenaces contre le biomédical : le domaine médical est également la cible d'attaquants.** En 2011, un ver a infecté le réseau d'un hôpital américain et a perturbé ses services. En Nouvelle-Zélande, 90% des transports médicalisés ont été immobilisés car 3 centres de communication avaient été touchés par un virus. Lors de la Black Hat, un expert a montré qu'il était possible de prendre le contrôle d'une pompe à insuline à distance.

- **Les SCADAs, les services de secours, les systèmes d'arme : tous ciblés par les *hackers*.** Les SCADAs continuent d'être en 2011 une cible privilégiée des *hackers*. Après Stuxnet, Duqu a pris le relais dans un rôle plus de renseignement que de sabotage visant le programme nucléaire iranien. Aux Etats-Unis, plusieurs infrastructures liées à l'eau potable ont subi des intrusions informatiques. En cause : les interfaces d'administration de ces systèmes critiques, accessibles via Internet et souvent très mal protégées (mot de passe faible). Les serrures IP, utilisées notamment dans certaines prisons, seraient également vulnérables à des attaques provenant d'Internet.

L'intégralité de la conférence ainsi que le support PowerPoint du Panorama sont disponibles en vidéo sur le site du CLUSIF mais réservés à ses adhérents.

Souveraineté des données et *cloud computing*

Le 22 décembre dernier, Dassault Systèmes se retirait d'Andromède, le grand projet de *cloud computing* souverain français, emportant avec lui son investissement potentiel de 60 millions d'euros[1]. Une décision qui intervient alors que la garantie de la propriété, de la sécurité et de la souveraineté des données est devenue un enjeu clé pour les entreprises, et surtout les Etat, ayant décidé de dématérialiser leur système d'information dans « le nuage »[2]. Une décision qui souligne aussi que si les Etats sont de plus en plus nombreux à tenir compte du *cloud* dans leur stratégie de protection des données, seuls certains réunissent les critères objectifs nécessaires au déploiement d'une véritable stratégie de *cloud* souverain.

Les Etats doivent en effet non seulement disposer d'infrastructures solides (*datacenters*, connectivité, etc.), de prestataires *cloud* proposant des offres compétitives mais aussi d'un cadre législatif et réglementaire leur permettant de conserver la mainmise, à la fois sur les données hébergées sur leur territoire et sur leurs données nationales stratégiques hébergées à l'étranger.

Des données éparpillées dans le monde

L'un des objectifs du *cloud computing* est d'abstraire l'infrastructure physique d'un système d'information. Ainsi, les données d'un client en France peuvent être stockées dans la même ville ou à plusieurs milliers de kilomètres à différents endroits, sans que cela n'affecte les performances perçues par l'utilisateur. Ceci permet de délocaliser chaque fonction du système là où l'infrastructure et le prix sont plus avantageux (régions polaires pour des gros *datacenters*, etc.).

Des infrastructures globalement prêtes pour le *cloud*

Le recours croissant au *cloud computing* fera augmenter de manière exponentielle la consommation d'électricité par les *datacenters*. La détention de fortes capacités en production d'électricité est donc un critère essentiel à la mise en œuvre de *clouds* souverains.

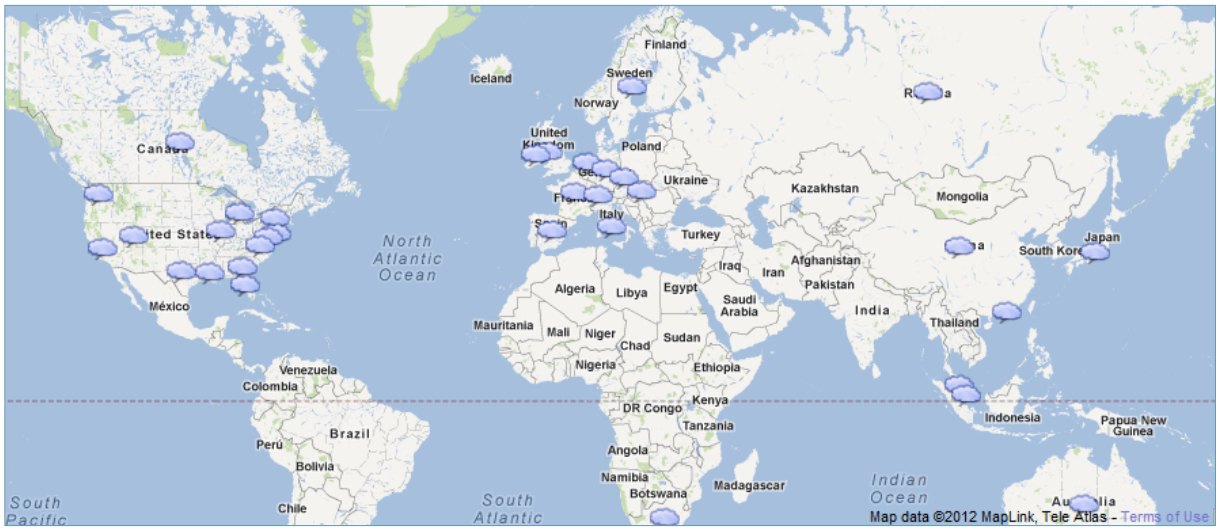
Le *cloud computing* exige également une certaine qualité d'infrastructure technique et de connectivité en-deçà de laquelle il ne pourrait pas fonctionner correctement. Certaines applications gourmandes en connectivité nécessitent en mode *cloud* du très haut débit et une proximité des *datacenters* afin de bénéficier de temps de réponse (ping) faibles.

La modernisation du réseau Internet aux Etats-Unis, en Europe et dans certaines parties d'Asie permet de mettre à disposition du *cloud* des bases techniques performantes et fiables. D'après le plan de *datacentermap.com* ci-dessous, les zones géographiques ayant le plus de fournisseurs de *cloud* se recoupent

[1] http://www.latribune.fr/technos-medias/informatique/20111222trib000673050/dassault-systemes-claque-la-porte-du-*cloud*-computing-a-la-francaise.html

[2] http://www.marketing-professionnel.fr/tribune-libre/*cloud*-computing-outil-competitivite-entreprises.html

logiquement avec celles dont la connectivité Internet est performante[3] : l'Amérique du Nord, l'Europe centrale et l'Asie.



Source : http://www.datacentermap.com/cloud.html

L'infrastructure et la connectivité dont nous disposons permettrait donc un développement acceptable pour certains services de *cloud* en Europe.

Cisco va plus loin dans son livre blanc « *Cisco Global Cloud Index : Forecast and Methodology* »[4]. En analysant les caractéristiques techniques d'Internet dans les différentes régions du monde, les ingénieurs de Cisco concluent que toutes disposent d'une infrastructure permettant un accès au *cloud* « basique », tandis que seules certaines régions seraient équipées pour en faire un usage avancé : l'Europe Centrale et Europe de l'Est, l'Europe Occidentale, et l'Amérique du Nord.

Un panel d'offres et un marché très disparates

Les bénéfices d'une architecture en *cloud* sont multiples. L'externalisation partielle ou totale du système d'information d'une administration ou d'une entreprise et la flexibilité des produits dits « *as-a-service* » font considérablement baisser les coûts de n'importe quelle infrastructure IT, ce qui rend ce marché considérablement dynamique.

Les américains ont été les premiers à se pencher sur ce domaine, notamment grâce à Amazon[5] et son offre AWS, utilisée par des centaines de milliers d'entreprises et quelques administrations dans plus de 190 pays[6], et les services *PaaS* de Google[7]. Plusieurs entités publiques américaines utilisent le *cloud* pour leur infogérance : la Defense Information Systems Agency, le Department of Energy, la NASA, le National Institute of Standards and Technology, entre autres. L'investissement total du gouvernement américain dans la migration vers le *cloud* est

[3] Pour plus d'informations sur les qualités d'infrastructures et de connectivité propres à chaque pays, consulter le Rapport Annuel OGI 2012.
[4] http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns1175/*Cloud*_Index_White_Paper.pdf
[5] http://www.businessweek.com/magazine/content/06_46/b4009001.htm
[6] http://aws.amazon.com/what-is-aws/
[7] http://www.guardian.co.uk/technology/2008/apr/17/google.software

de 20 milliards de dollars[8], ce qui représente 25% du budget total accordé aux TIC. Les prédictions indiquent que le marché privé passera de 41 milliards de dollars en 2011 à 241 milliards en 2020[9].

Si les offres américaines sont abouties, le marché européen du *cloud* souverain en est à ses balbutiements. La France a par exemple lancé Andromède, projet de 285 millions d'euros[10], financé en partie par France Télécom/Orange et Thalès. La Direction de l'information légale et administrative (DILA) souhaite aussi un *cloud* privé, qu'elle créera en partenariat avec Accenture. Le Royaume-Uni a quant à lui publié sa stratégie de *cloud* gouvernemental, visant à économiser 340 millions de livres d'ici à 2015[11].

En Asie, la Chine compterait investir 154 milliards de dollars[12] dans un *cloud* public. Elle a été classé 8ème parmi les pays prêts à accueillir le *cloud*, derrière le Japon (1er) et Hong Kong (2ème)[13], ce dernier étant l'un des principaux *« hubs »* du *cloud computing* en Asie. Les pays asiatiques voient le *cloud* comme une réelle opportunité commerciale au plan mondial. La Russie a quant à elle déclaré vouloir investir plus modestement, reconnaissant que le marché était aujourd'hui très largement tenu par des acteurs américains. Son *cloud* public sera financé à hauteur de 4 millions d'euros en 2011 et la mise serait doublée en 2012 – 2013[14].

La souveraineté des données dans le *cloud*

Le *cloud computing* place la question de la souveraineté des données au cœur du débat. Quel est le sort des données stratégiques d'une administration dont l'infogérance est externalisée sur un *cloud* hébergé à l'étranger ? Qui aura la mainmise sur ces données ?

Les Etats-Unis semblent bénéficier de tout le dispositif nécessaire au déploiement d'offres de *cloud* : des prestataires aux offres matures, les infrastructures nécessaires pour accueillir bon nombre d'administrations ou sociétés à des prix très compétitifs. Mais le marché étranger (et notamment européen) leur est de plus en plus imperméable : les acteurs européens sont réticents à externaliser leurs données vers des *clouds* américains, la souveraineté de leurs données stockées y étant remise en cause.

Le PATRIOT Act signé en 2001, suite aux attentats du 11 septembre 2001, donne aux autorités américaines un contrôle complet sur la totalité des données stockées ou transitant sur leur sol[15] lorsque ces éléments sont en lien avec des activités d'espionnage ou de terrorisme (sections 215 et 806). Des perquisitions et saisies peuvent également être réalisées pour des actes de contrefaçon commis dans le cadre d'une organisation criminelle[16], comme dans l'affaire « Megaupload ». La souveraineté des données est donc assurée *de facto* pour les américains sur leur sol.

Mais la problématique latente du PATRIOT Act[17] s'étend à l'international : tous les services de *cloud* américains (y compris Amazon et Google) sont soumis à cette loi. De fait, les données confidentielles de gouvernements étrangers hébergées dans un *cloud* américain se retrouvent potentiellement accessibles par le gouvernement américain, ce qui dissuade fortement les potentiels clients étrangers de souscrire à des offres de *cloud*

[8] http://www.cio.gov/documents/federal-*cloud*-computing-strategy.pdf
[9] http://www.politico.com/news/stories/1111/69366.html
[10] http://www.lemondeduc*loud*.fr/lire-285-millions-d-euros-pour-andromede-le-*cloud*-souverain-francais-41990.html
[11] http://www.cabinetoffice.gov.uk/sites/default/files/resources/government-*cloud*-strategy_0.pdf
[12] http://www.computerworlduk.com/news/cloud-computing/3303458/china-to-invest-98-billion-in-cloud-computing/
[13] http://www.asia*cloud*.org/index.php?option=com_content&view=article&id=160
[14] http://internetno.net/category/biznes/analitika-biznes/gosudarstvennye-oblaka-idut-v-rost/
[15] http://www.aclu.org/files/FilesPDFs/patriot_text.pdf
[16] Voir : Affaire Megaupload : http://www.journaldunet.com/ebusiness/expert/50873/fermeture-du-site-megaupload---quels-enseignements-pour-le-cloud-computing.shtml
[17] http://www.npr.org/news/specials/patriotact/patriotactdeal.html

américaines[18]. En Allemagne[19], T-Systems utilise même le PATRIOT Act et la souveraineté de ses données comme des arguments de vente[20].

La réflexion sur la souveraineté des données se traduit aussi à l'échelle européenne. Les récents travaux de la Commission Européenne de Justice représentée par Viviane Reding ont mené à la mise à jour de la législation de 1995 sur la protection des données des citoyens européens[21]. Elle souhaite harmoniser les législations nationales et garantit un « droit à l'oubli » pour les données de citoyens européens, même si leurs données se trouvent géographiquement dans un pays non-membre de l'UE. Cette législation, bien qu'encourageante, pourrait tarder à entrer en vigueur.

Ne voulant pas rester en retrait par rapport au marché mondial du *cloud*, la Chine compte inclure une « Cloud Zone » dans son programme de *cloud*. Cette zone serait exempte du filtrage du « Great Firewall » Chinois, ce qui permettra aux personnes qui y travaillent d'accéder à Internet sans censure[22]. Cette décision vise notamment à améliorer le classement de la Chine dans le « Cloud Readiness Index », où sa politique de protection des données lui confère un mauvais score.

Vers le protectionnisme des données et la réapparition des frontières ?

La politique de protection des données peut varier énormément de pays en pays (voire d'Etat en Etat, dans le cas d'un Etat fédéral comme les Etats-Unis). En dépit de toute l'abstraction que le *cloud* permet, les données qui y sont stockées doivent bien exister quelque part et avoir une localisation géographique précise.

Avec l'apparition de législations basées sur des critères géographiques, comme le PATRIOT Act, la question de la localisation des données, à laquelle les utilisateurs souhaitent se soustraire, redevient primordiale. L'abstraction technique et logique oblige donc à disposer de réponses concrètes dans le domaine légal. De même, la question peut se poser par rapport à la nationalité des sociétés hébergeant le contenu : une société américaine en France est-elle sujette aux mêmes lois qu'une société française ?

Le problème se complexifie dès lors que se fait la distinction entre fournisseurs d'infrastructure (serveurs physiques), prestataires de service (couche « logique » du *cloud*) et clients. Dans le *cloud*, il est fréquent que les trois acteurs ne soient pas au même endroit. Des études indiquent cependant que ces entreprises pourraient appartenir à un nombre restreint de grands acteurs[23].

Le problème est d'autant plus prégnant qu'il n'existe pas encore de solution concrète, même si la législation européenne annoncée le mercredi 25 janvier 2012 est un pas important dans la sauvegarde de la souveraineté des données en Europe. Dépourvue de régime juridique consensuel adapté, la technologie *cloud* pourrait très bien faire l'objet d'une forte régionalisation et se cantonner à des marchés très localisés, où chaque changement législatif représenterait une nouvelle barrière à franchir. Autant de contraintes qui n'étaient pas prévues dans le paradigme initial du *cloud*.

[18] http://www.politico.com/news/stories/1111/69366.html

[19] Voir « Bundesdatenschutzgesetz », loi allemande de protection des données - http://cloudnod.com/2010/01/the-german-data-protection-act-bdsg-and-cloud-computing-in-2010/

[20] http://www.bloomberg.com/news/2011-09-13/deutsche-telekom-wants-german-*cloud*-to-shield-data-from-u-s-.html

[21] http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/11/762&format=HTML&aged=0&language=FR&guiLanguage=fr

[22] http://www.penn-olson.com/2011/06/23/china-*cloud*-zone-no-firewall

[23] http://bits.blogs.nytimes.com/2012/01/30/here-come-the-*cloud*-cartels/

	Etats Unis		France	
	Programme officiel GVT	**Armée**	**Andromède**	**Dila**
Stratégie globale	Oui, officielle	-	-	-
Public / privé	Privés (entités gouvernementales uniquement)	Privé (Army uniquement)	Public, puis à l'Europe (future législation surement nécessaire)	Privé
Acteurs concernés	NASA, Administration, entités, etc.	Armée (Air force, etc.)	Entreprises privées	Dila (journal officiel, services d'information citoyens, débat publique, diffusion légale)
Budget	20 B $ (sur 80 B $)	250 M $ (pour cloud privé)	285 M €	-
Avancement	Opérationnel, migration en cours	Migration en cours	Retardé par l'abandon de Dassault	Prêt pour mars 2012
Législation spécifique	Patriot Act	NDAA, contraints à utiliser un *cloud* tiers	Loi informatique et libertés	
Souveraineté des données	Oui, tout est hébergé sur le territoire national	Oui, efforts d'indépendance par rapport aux solutions commerciales	Oui, raison d'être	Oui, envergure nationale
Fournisseurs d'infrastructures et prestataires	Google, IBM, HP, etc.	Compagnies non spécifiées, mais veulent être indépendants	Orange, Thales, Cap Gemini	Accenture, Cisco, NetApp et VMware

	Royaume-Uni	Allemagne	Chine	Russie
	Gcloud	**Trusted Cloud**	**Cloud Zone**	**Cloud administratif**
Stratégie globale	Oui, officielle	Oui, officielle	Oui	Oui
Public / privé	Privé	Hybride	Public	Privé
Acteurs concernés	Gouvernement et administration	Services administratifs	Startups, gouvernement	Services administratifs
Budget	340 M £ d'économies	50 M €	154 B $	4 M €, deux fois plus en 2012 - 2013
Avancement	Opérationnel pour mars 2012	Début de recherche	En construction	En construction
Législation spécifique	-	German Data Protection and Privacy Laws	Oui, "Cloud Zone"	Loi laxiste quant à la protection des données
Souveraineté des données	Non. Mais notion d' « Information Assurance »	Oui, très forte	Oui, s'efforcent de s'adapter aux exigences étrangères (censure)	Non
Fournisseurs d'infrastructures et prestataires	Accenture, Cisco, BT	-	Acer et Philips	-

	Japon	Thaïlande
	Kasumigaseki Cloud	**Cloud gouvernemental**
Stratégie globale	Oui	Oui
Public / privé	Privé	Privé
Acteurs concernés	Services administratifs	Services administratifs
Budget	-	1.6 M $ (pour les tests)
Avancement	Achevé en 2015	Tests en mars 2012, lancement en avril
Législation spécifique	-	-
Souveraineté des données	Non	Non
Fournisseurs d'infrastructures et prestataires	-	TOT *public company*, CAT Telecom, et divers fournisseurs mobiles

IDC Sécurité IT	Paris	Le 8 février 2012
DOJ Cyber Security Conference	Washington D.C. (USA)	Les 8 et 9 février 2012
Security & Safety Technologies Moscow	Moscou (Russie)	Du 14 au 17 février 2012
RSA Conference	USA	Du 27 février au 2 mars 2012
Secutech India	Bombay (Inde)	Du 1er au 3 mars 2012
Black Hat 2012	Amsterdam (Pays-Bas)	Du 14 au 16 mars 2012
2nd annual Cyber Security China 2011	Péking (Chine)	Du 22 au 23 mars 2012
IST International Forensic Technologies Fair	Varsovie (Pologne)	Le 28 mars 2012
HackCon	Oslo (Norvège)	Du 26 au 29 mars 2012

La Délégation aux Affaires Stratégiques propose les analyses politiques et stratégiques contribuant à renforcer l'appréciation des situations et l'anticipation.
Elle soutient la réflexion stratégique indépendante, en particulier celle menée par les instituts de recherche et organismes académiques français et étrangers. Elle contribue au maintien d'une expertise extérieure de qualité sur les questions internationales et de défense.
A ce titre, la DAS a confié à la **Compagnie Européenne d'Intelligence Stratégique (CEIS)** cet Observatoire du Monde Cybernétique, sous le numéro de marché 1502492543.
Les opinions développées dans cette étude n'engagent que leur auteur et ne reflètent pas nécessairement la position du Ministère de la Défense.

Ministère de la défense et des anciens combattants
Délégation aux Affaires Stratégiques
Sous-direction Politique et Prospective de Défense
14 rue St Dominique 75700 PARIS SP 07

CEIS
Contact : Guillaume TISSIER
Téléphone : 01 45 55 00 20
Télécopie : 01 45 55 00 60
E-mail : gtissier@ceis.eu

Retrouvez cette lettre et l'ensemble des articles cités sur l'extranet de l'OMC à l'adresse suivante (accès soumis à authentification) :
https://owldesk.ceis.eu/